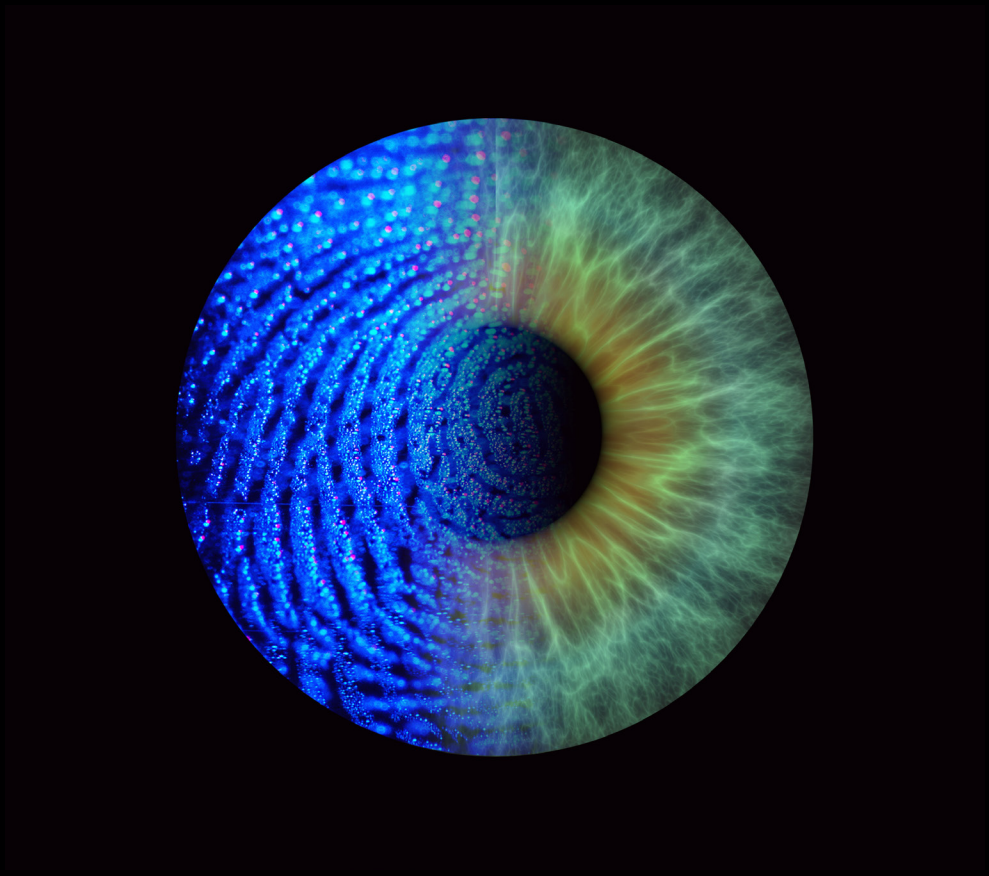
Deloitte.



Continuous fraud monitoring and forensic investigations

Acknowledging and addressing the risk of being blindsided

A whistleblower's hotline call prompts a bid-rigging investigation. Payroll analysis finds ghost employees lurking in the ranks. A vendor audit points to a possible kickback ring. Whether internal or external, successful or thwarted, a fraudulent act compels an organization to address critical questions. Who all is involved? What has the scheme cost us? How long has it been going on?

Recent Deloitte POVs have discussed key dimensions of an organization's analytics-driven fraud-fighting approach: the role of analytics, the need for available and accurate data, and the technologies required to extract and realize data's value. Another critical component of fraud defense, one that can help address the questions above, is continuous monitoring of transactions and activities. Organizations that use technology to monitor for potential risks, as well as analytics to identify new emerging threats, may be better positioned to mitigate the blind spots in their fraud defenses and address the risks of being blindsided financially, operationally, and legally.

The challenges in combating fraud

The longer fraud perpetrators go undetected, the greater financial harm they cause. And, recovery becomes more difficult with time. The duration of typical schemes amplifies the need for continuous monitoring to uncover threats. Research has found more than half of frauds continue at least 18 months before detection and nearly one-third go undiscovered for two years or more.

Various factors impede fraud detection and avoidance, including overwhelming data volumes, scarce forensic analytical skills, and the expense of needed technology and training. An organization that hires data scientists to conduct fraud analysis may discover they can crunch numbers but lack critical domain knowledge.

Often, fraud fighting is primarily reactive, with resources focused on chasing perpetrators after an incident, at the expense of detection and prevention. Internal audit, supply chain, and other functions may search for fraud in silos, missing opportunities for collaboration and information sharing. Risks may be monitored based on established criteria and past incidents, rather than using a more robust, data-driven approach that considers potential unknown threats.

Constantly advancing technologies create other concerns. The proliferation of digital devices increases efficiency and automation, but also elevates the organization's risk exposure as internal audit may fall behind the business units in technology deployment and expertise.

The nature and potential of continuous fraud monitoring

One might reasonably think of continuous monitoring as an automated process that flags suspicious transactions the moment they occur. The process may be rule-driven, for example producing an alert anytime a transaction exceeds a threshold amount or is processed outside of normal business hours.

Continuous, however, is a relative term in this context. Real-time, 24/7 monitoring may not be necessary or useful, especially in detecting complex fraud schemes. As noted, research has shown that frauds typically evolve over time. A single transaction may mean little, but monitoring the transaction trend on a monthly, weekly, or other basis could speak volumes.

Proactive monitoring that leverages advanced analytics can help organizations identify trends, as well as fresh schemes that aren't based on known instances of fraud. Rather than relying on rules, analytics produce new insights driven by what the data is showing.

Attention to several considerations can help an organization generate greater value from its monitoring activities:

Embrace the deterrent effect. People have a way of falling in line when they're being watched, whether by humans or machines. The mere existence of monitoring, properly communicated, can help nurture compliance with protocols, policies, and guidelines.

Keep it in house. Conducting monitoring within the organization instead of turning to an outside party offers several advantages, including data security and privacy. Data can be analyzed more easily on a continuous basis, and the in-house personnel can learn both how the solution works and how to maintain it. Plus, if the solution needs to be expanded in the future, the work can be done within the organizational infrastructure and not require additional data exporting.

Customize monitoring to specific risks. Disparate organizations, industries, and locations can present different exposures and threats. Data formats, complexity, and availability can vary widely. Understanding trends and tailoring fraud solutions to specific organizational characteristics and situations, with business unit involvement, can help capture greater value from monitoring activities.

Capitalize on available resources. Some of the tools needed to conduct monitoring may already exist within the organization in areas such as finance and supply chain. Opportunities may exist to leverage these investments for risk management. Such collaboration can also enhance communication among different parts of the business, further strengthening fraud awareness.

Use a range of approaches. Different risks can require different analytical tools. Unsupervised modeling creates statistical profiles of normal transactions or entities and identifies outliers from these profiles. Supervised modeling uses documented fraud cases and output from unsupervised modeling to learn fraud characteristics, classify new observations as fraudulent, and detect what human observation cannot. If an apparent scheme involves collusion, network analysis may be required. And, if important clues appear to lie in unstructured text, natural language processing may be a valuable approach.

Involve stakeholders. Risk management is no longer just the responsibility of internal audit and compliance. Business units and other functions have roles to play in identifying, understanding, and addressing fraud risks.

Focus the effort. Monitoring solutions are complex, touching disparate parts of the business. The investment and time required to implement them can seem overwhelming. Rather than casting a wide net, consider conducting a focused, specific proof of concept to understand how a solution works and the value it could potentially provide.

Stop chasing, start preventing

Establishing effective fraud monitoring can seem a monumental task, one requiring significant investment, a major implementation initiative, and huge effort to wrangle the needed data. It needn't be overwhelming, however.

Start by abandoning the idea that an ideal situation and perfect data are required. Deploying analytics is just element of a longer and broader enterprise risk management and compliance journey — a vital part, but just one nonetheless.

Next, conduct a current state assessment to determine where relevant data resides, as well as the infrastructure and tools available to house and carry out continuous monitoring. Then, define objectives, establish focus areas, and prioritize needs and actions.

With such an approach, monitoring capabilities can improve iteratively over time, yielding deeper insights, fewer false positives, and a resilient organization less vulnerable to being blindsided by fraud threats.

Contact us

Don Fancher
Global Leader|Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 770 265 9290
dfancher@deloitte.com

Ed Rial
Principal | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 212 436 5809
erial@deloitte.com

Satish Lalchand
Principal | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 202 220 2738
slalchand@deloitte.com

Shuba Balasubramanian
Principal | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@deloitte.com